Denver Law Review

Volume 79
Issue 4 *Symposium - Privacy*

Article 8

December 2020

Supremarket Cards: The Tip of the Retail Surveillance Iceberg

Katherine Albrecht

Supermarket Cards:
The Tip of the RETAIL SURVEILLANCE Iceberg

by Katherine Albrecht, Ed. M.
CASPIAN - Consumers Against Supermarket Privacy Invasion and Numbering[1]

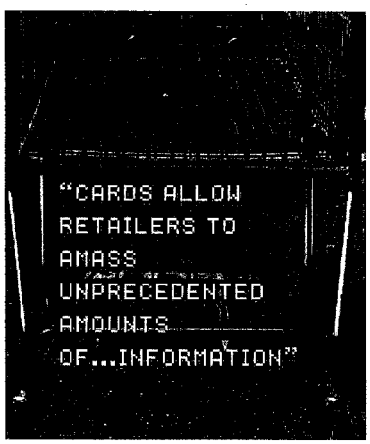
SECTION 1: INTRODUCTION AND BACKGROUND

The good news is, marketers know so much more about you that they can precisely tailor their marketing messages. The bad news is, marketers know so much more about you even when you would prefer your anonymity. One man's relevance is another man's intrusion. Big Brother has truly arrived, with a grin and a fist full of coupons.[2]

- Frequency Marketing in the 21st Century

Love 'em, hate 'em, or merely tolerate them, there is no escaping the fact that supermarket cards have become a fixture of the American retail landscape. Since first appearing in the early 1990's, card-based purchase tracking programs, variously known as loyalty, frequent shopper, reward, or club cards, have spread quickly throughout the grocery industry. In January 2000 it was estimated that 60% of U.S. grocers required a card to obtain discounts,[3] and today eight of the top ten U.S. grocery retailers own at least one supermarket chain with a card program in place or a trial underway.[4]

Promoted as savings devices by the grocery industry, cards allow retailers to amass unprecedented amounts of longitudinal information on consumer purchase and eating habits. Each time a shopper scans a card at the checkout lane, a record of the items purchased, the time, the store location, and the payment method are added to the shopper's profile. Along with millions of other records, this profile is stored in an enormous "data warehouse" (frequently a secure facility run by a marketing company under contract to several different supermarkets) where it can be analyzed in detail or simply stored until a later use is found for it.



A storm on the horizon

...she has resigned herself to those moments of simmering anxiety she sometimes feels when she hands over her card at the grocery store. 'It's like sitting in your beachfront property watching the storm warnings, hoping the hurricane doesn't hit you,' said Arden Schell, 58, of Arlington. 'It's the kind of thing you worry about but you don't know how to put a stop to it.'[5]

- Robert O'Harrow, Jr., Washington Post Reporter, quoting Virginia Shopper Arden Schell

Though the majority of American households have signed up for at least one supermarket card,[6] high rates of program participation do not necessarily mean that consumers are comfortable with the programs. A growing segment of the population has begun to express deep concerns about the privacy implications of using supermarket cards.

Shoppers like Arden Schell are correct in sensing a storm on the horizon. Today, not only can marketers and product manufacturers access a dizzying array of data on supermarket shoppers through the use of cards and related technologies, but soon social agencies, health insurance companies, law enforcement, the

United Nations, criminals, and lawyers may also begin clamoring for their own up-close view of shoppers' personal food shopping habits.

By allowing their grocery purchases to be tracked and recorded, consumers leave themselves vulnerable to threats from these sources. This article sets out to document these risks and provide information to enable shoppers to make informed decisions about whether or not to participate in supermarket card programs.

Why fight supermarket cards?

The food business is far and away the most important business in the world. Everything else is a luxury. Food is what you need to sustain life every day. Food is fuel. You can't run a tractor without fuel and you can't run a human being without it either. Food is the absolute beginning.

- Dwayne O. Andreas, Former Chairman of the Board, Archer Daniels Midland Company

At first glance it may seem odd that a privacy researcher would conduct an in-depth analysis of something as mundane as supermarket cards, especially considering how many other invasive technologies have sprung up in the last decade. But while other privacy-violating technologies may be flashier, few have the pervasive reach of the lowly grocery card. Virtually every American family patronizes a supermarket,[8] and since food is essential for survival, obtaining it is perhaps the least negotiable of consumer activities. Supermarket practices arguably have greater potential to impact society than those of any other retail channel.

The grocery cards in their wallets provide many shoppers with their first glimmer of awareness about retail surveillance. Though the most egregious privacy violations in the commercial sphere occur far from the average consumer's experience and awareness, grocery cards provide tangible evidence of their existence. Tracked back to their source, the cards lead the investigator to a staggering host of complex strategies to watch, record, and control consumers on an enormous scale.

Background of supermarket card programs

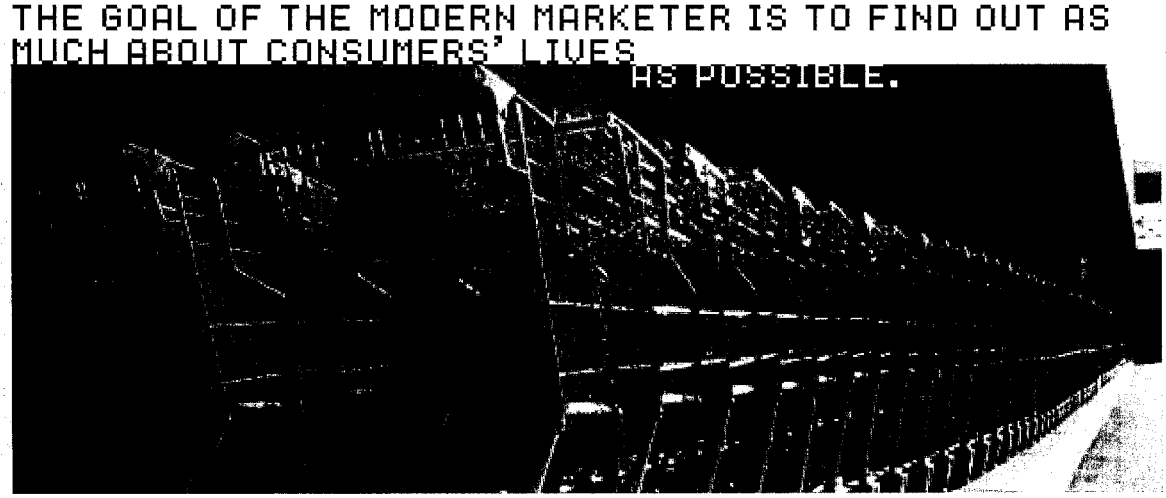
Loyalty schemes are not gestures made by philanthropic superstores.[9]

- Mark Price, Waitrose Supermarket Executive

Understanding how supermarkets have come to embrace the card concept can provide a framework for understanding the privacy implications of cards. The goal of the modern marketer is to find out as much about consumers' lives as possible. In the past, marketers were frustrated by the fact that many consumers do not want to provide information about themselves to strangers. Marketers had to pay for people to provide them with information about their purchases (a fair arrangement based on mutual consent), but since the industry could not to afford to pay all American shoppers to be tracked, for years it limped along with what it could glean from the occasional survey or focus group.

Then the marketers hit on an idea. Rather than use money as the carrot to entice people into surrendering private information about their shopping habits, they could use it as a stick to punish people into surrendering that information. And what's more, if they did it right, consumers might never be the wiser.

Fast forward ten years, and here we are — the supermarket card is a fixture in virtually every shopper's wallet. By withholding access to sale prices, marketers have coerced tens of millions of Americans into surrendering data that they would never have revealed voluntarily. Even though discounts on overstocked and seasonal items have been around for thousands of years, shoppers can now only receive discounted prices if they comply with the supermarket's surveillance agenda by serving as unpaid research subjects. And punishment for refusal (the stick) is harsh: anyone refusing to participate is penalized in the form of higher prices — sometimes to the tune of double or more for a given grocery item.[10]



It's brilliant that the marketers didn't have to give anything up in the process. Ostensibly, the cards are designed to save shoppers money, so participating consumers should see their grocery bills drop significantly as soon as the programs are implemented. However, when prices at Kroger were compared before and after the introduction of a card program in Indiana in 2000,[11] exactly the reverse was found to be true — sale prices on identical items went up after the cards. Nevertheless, given a choice between mediocre discounts with the card, or no discounts at all without it, most consumers capitulate and sign up.

Consider how many shoppers would still choose to be monitored if there were no punishment for refusal, and the motivating factor (the stick) quickly becomes apparent.

The industry talks out of both sides of its mouth

On the surface, customers view the card as a tool to receive discounted prices or other incentives. Marketers, on the other hand, use the cards to learn about their shoppers.[12]

- Ann Raider, Marketing News

Most people, amazingly enough, look at what's going on with that card and don't connect that we have the data. For those of you in this room [MIT media lab] I have no doubt that you know we have access to data on you. But for a lot of consumers, it's a frightening thing.[13]

- Curt Avallone, VP of Marketing and New Technology, Stop & Shop Supermarket

While industry trade publications openly discuss the data collection function of cards, the supermarkets carefully avoid mentioning data collection to customers. Instead cards are promoted through advertising and promotional materials as "savings" devices to "reward" loyal shoppers.

Shoppers are intentionally kept unaware of the privacy implications associated with cards. When first announcing its involvement with the supermarket loyalty card concept a few years back, Catalina Marketing Corporation (CMC) hired a public relations agency, the CGI Group of New York, to "minimize media coverage linking CMC with unethical obtrusive database marketing."[14]

CGI proudly stated on their website that "despite questions from the press regarding privacy issues not one resulting story mentioned the (privacy) issue."[15] The campaign to squelch discussion of privacy within the media, coupled with extensive advertising, served to keep these concerns from many shoppers' awareness in the initial phases of card introduction in this country.

Unfortunately, many shoppers only discover that the card is a data collection device (rather than a savings device) after several months — or even years — of regular use. By that time the store has already collected a large dossier of information on the individual and for many shoppers it feels too late to complain. Though many people then contact the stores asking to have their records expunged (only to be told in most cases that their data is now the property of the store), most consumers simply accept the situation as an unfortunate *fait accompli* since to do otherwise would require admitting to their previous ignorance and explaining a history of "voluntary" card usage.

Consumer acceptance levels are debatable

Because many studies on consumer acceptance levels of supermarket cards have been commissioned or conducted by companies with a financial stake in the outcome, it is difficult to gauge the true acceptance levels for cards among consumers. Independent research is needed to accurately determine how consumers feel about data collection, price considerations, and other factors that play a role in consumer card usage. When asked, grocery executives point to internal surveys as evidence that consumers support their card programs.[16] Indeed, it is probably true that if store representatives ask shoppers, "Would you use a loyalty card if it meant you could save money on your groceries?" many may well answer yes. However, consider the results if a survey were to ask this, more truthful question:

> If your supermarket required you to provide personal information and carry a card to be eligible for sale prices (the same sale prices you already get today), and furthermore, used that card to make a record of all of your purchases in perpetuity with the goal of extracting more money from you, leaving you no way to manage or expunge that record and leaving it vulnerable for use against you in a variety of ways, would you approve?

The majority of shoppers would probably answer with an emphatic and resounding "NO!"

SECTION 2: USE AND ABUSE OF SUPERMARKET DATA

Can supermarkets be trusted with data?

Whenever concerns about data collection are raised, supermarkets point to their privacy policies, particularly their promise not to share card data with third-parties. Despite this promise, many chains routinely sell large amounts of card purchase data to outside marketing and manufacturing companies, justifying this practice on the grounds that they remove "identifying information" before sharing the records. But is shopper card data, minus a name and address, really anonymous?

Data reidentification

A computer process called "reidentification" can allow marketers to re-attach names and addresses to "anonymous" records — even after all so-called "identifying information" has been removed.[17] The process works by combining the "anonymous" data set with outside information to pair up items that are uniquely associated to individuals. For example, using only birth date and full ZIP code it is possible to identify 97% of the Cambridge, Massachusetts population.[18]

The U.S. General Accounting Office recently expressed alarm over the reidentification trend which it says enables

marketers and other "data snoopers" to identify specific individuals on the basis of very limited information.[19] The U.S. Census Bureau is so concerned about reidentification by marketers that it recently took pains to "blur" census records before releasing them.[20]

Unfortunately, the average supermarket IT department is unlikely to invest in complex and expensive "blurring" procedures before selling "anonymous" or "aggregate" shopper card purchase information to data-hungry marketers, meaning that your personal information could easily fall into the marketers' hands. Researchers predict that reidentification risks will increase as the amount of data available on individuals continues to grow.[21]

Internal risks

Unbeknownst to most shoppers, the information contained in their supermarket card records may extend far beyond mere grocery purchases, name, address and phone number. In the early stages of card introduction, many stores required a social security number or driver's license number (or both) to receive discounts — and would not issue a card without them.[22] Today, because many stores' shopper cards double as "check cashing cards," such identifying information is still routinely collected from millions of grocery consumers without raising an eyebrow. Even shoppers who do not want check cashing privileges are often encouraged to provide additional information, such as their date of birth, on card applications.

The problem is that once the store has shoppers' identifying information, it can easily obtain detailed intelligence on other aspects of their lives. A Florida company, AccuData, aggressively markets a product it calls a "penetration profile" to grocers.[23] These profiles are designed to augment the grocery purchase data collected on customers with a wealth of additional information about them from outside databases.[24] AccuData recommends that supermarkets attach the profiles to customer data files so they can better analyze the "geodemographic, psychographic and purchasing characteristics" of their unsuspecting customers.[25]

Data collected in this way not only violates customers' expectation of privacy, but it is also subject to internal security risks. The IT staff of a typical supermarket has access to all information contained in the store's shopper card records. This data is often held on insecure computer systems where even low-ranking employees have access. Here it is subject to both human error and employee corruption.

On the error front, stories abound of sensitive personal data stored on corporate computers being accidentally revealed to the public. One recent case involved Travelocity.com inadvertently posting the names, addresses, phone numbers, and e-mail addresses of 45,000 customers on its website for a period of several weeks before the error was discovered.[26] On the corruption front, it was recently alleged that AOL employees have been providing criminals with subscribers' passwords and account information to make fraudulent purchases.[27] One hacker said, "AOL's biggest security risk is corrupt employees who will straight up give away info for a price."[28]

There are also a number of disquieting cases where Internet companies reneged on their privacy policies during hard times by attempting to sell customer purchase data to the highest bidder (e.g., Toys.com[29] and Voter.com[30]). Companies have also retroactively eased privacy restrictions to allow them to reveal previously collected customer data (e.g., Amazon.com,[31] e-Bay,[32] and Yahoo[33]).

These are only the publicly reported cases. Larry Ponemon, a privacy expert who has conducted hundreds of corporate privacy audits both for PricewaterhouseCoopers and later as an independent privacy consultant,[34] reports that only 19% of financial businesses actually adhere to their privacy policies.[35] The reality is that whenever sensitive data is collected there is always a risk that it can be revealed in error, misused, or abused — and privacy policies offer little protection against these threats.

Personal injury and family law

Shopper cards have already begun cropping up in personal injury and family law cases. A California shopper named Robert Rivera sued Safeway-owned Vons supermarket after slipping on a yogurt spill in the store and fracturing his kneecap.[36] A mediator allegedly told Rivera's attorney, M. Edward Franklin, that Vons planned to introduce Rivera's liquor purchase records at trial to paint him as an alcoholic.[37] In another case, a man's supermarket card records indicating purchases of expensive wine were used against him in a divorce proceeding as evidence that he could afford to pay more alimony than he had claimed.[38]

Other security risks

The keychain versions of supermarket cards pose their own security risk. Anyone finding a shopper's keys has the potential to gain access to the data linked to it. Stop & Shop Supermarket in Boston gave a customer's name, unlisted home phone number, and residential address to a complete stranger who had found the customer's keys using the shopper card number on the key chain card.[39] The potential for danger is obvious if a criminal has the key to a person's front door and knows both his or her address and phone number.

In late 2001, a radio producer in Dallas obtained similar information from Safeway-owned Tom Thumb Supermarket.[40] She called Tom Thumb's toll free customer service line claiming to be a stranger who had found a set of keys in the parking lot (though they were actually her own). The customer service representative used the customer number from the key chain tag to quickly obtain her name and home address, which he then freely gave out to her (a supposed stranger) over the phone.[41]

Tom Thumb later apologized for the incident, explaining that the employee had made an error by sharing the information.[42] However, the company's explanation simply

underscores the point that no retailer can guarantee human error will not lead to disclosure of customers' personal information.

Shopper card records and health

HMO's may soon have shopper card data

Supermarket cards record more than just purchases; they make a record of the actual food people put into their bodies. Because they contain nutritional information for tens of millions of Americans, supermarket databases offer a potential gold mine for anyone who wants to monitor the eating habits of individuals and groups of people.

One U.S. supermarket chain, Royal Ahold-owned Stop & Shop, has already poured $3 million into the development of a very disturbing software program called SmartMouth to tap this potential.[43] SmartMouth can sift through the millions of supermarket card records Stop & Shop has collected on shoppers over the past eight years to create nutritional profiles on each individual cardholder.[44] If a customer has been overindulging in sugar and fat or ignoring a doctor's warning to cut back on sodium, the supermarket — or anyone else with access to the database — can find out with just a few mouse clicks.

While Stop & Shop has temporarily shelved the program, its future plans for SmartMouth are perhaps the most alarming I have yet encountered with regard to shopper cards: Stop & Shop executive Curt Avallone recently made the shocking admission that his company is considering "an HMO alliance" with "three or four health organizations" to make use of the SmartMouth program and Stop & Shop customer records.[45]

The staggering potential to form longitudinal nutritional profiles on their subscribers is not lost on health insurance companies, who could use the information to deny coverage, set rates, or use a person's lifetime eating habits to deny medical procedures such as heart bypass operations and dialysis. HMO subscribers' medical records and their food purchase records could become so intertwined that eating habits could ultimately become part of a patient's standard medical chart.

Stop & Shop is not the only company that has expressed an interest in linking card data to health records. Boots, a major British pharmacy retailer, offers medical and dental insurance plans linked to its "Advantage Card,"[46] which can also serve as a chip-based credit card.[47] Boots even encourages shoppers to donate their organs through a check box at the bottom of the card application, explaining on their website that "joining through Boots provides you with a combined Advantage Card and Organ Donor scheme card in one plus the peace of mind that your donor details are safely stored on the NHS [National Health Service] Organ Donor Register."[48]

Boots hopes to someday link its frequent shopper card with customers' medical records, health insurance, and social security information,[49] and the "smart card" industry here in the U.S. is clamoring for the same thing.[50]

The use of shopper card records to track health problems could be of interest to some members of the legal community, who have begun contemplating class-action suits against snack food companies.[51] Both attorneys and food manufacturers may soon develop a keen interest in who bought what, when, and in what quantities, along with individuals' health records to either instigate or fend off lawsuits.

If shopper card records are allowed to evolve into de facto health records, they will become an obvious target for government agencies wishing to claim their own piece of the information pie. Already, a chip-based "Health Passport card" (which uses a microchip to store and retrieve health information and "redeem nutrition benefits") has been issued to welfare recipients in three U.S. cities.[52] Disturbingly, the card, which is required to purchase groceries under the Women, Infants and Children (WIC) program, links food purchase information with medical assessments, health records, and immunization records, thus allowing WIC officials to closely scrutinize the nutritional makeup of a family's weekly shopping.[53] Observers in Wyoming, one of the program's test locations, say that eventually the Health Passport program could be expanded to include all citizens in the state, not just those receiving public assistance.[54]

Government health organizations want access to shopper card records

Anything recorded is subject to control.
- Katherine Albrecht, CASPIAN[55]

"Public health" has already been used as justification for three British supermarket chains to violate their privacy policies by offering card records to the government. With very little prompting, these chains agreed to release shoppers' purchase records to health officials to track the consumption and health effects of genetically modified (GMO) foods.[56] The study, which was fortunately cancelled, had planned to link store records and health databases seeking links between GMO food purchases and a variety of health problems, apparently without obtaining the permission of the shoppers concerned.[57]

Scottish health officials would like access to shopper card records to facilitate "the monitoring and evaluation of the various initiatives to promote improved [Scottish] diet."[58] Calling such data "invaluable," their report says that they plan to "consult the major supermarkets to explore the feasibility of accessing this data and to examine with them the scope for other uses to which loyalty card data might be put."[59]

Most worrisome of all, the World Health Organization (WHO) recently stated that one of its major objectives is to "*maintain global databases* for monitoring, evaluating, and reporting on the world's major forms of malnutrition, the effectiveness of nutrition programmes, and progress towards achieving targets at national, regional and global levels."[60] The global database would be a component of the WHO's larger plan

to "prevent, reduce and eliminate malnutrition worldwide,"[61] implying that the WHO envisions a more active role for itself in the global food arena than the mere collection and analysis of data. Will the United Nations someday demand shopper card records from around the world to form the basis of the WHO's "global database"?

Regardless of the good intentions of health officials, it is imperative that citizens keep grocery records out of government hands. Allowing governmental bodies to monitor and evaluate citizens' purchase and consumption of food could lead to various forms of control over the food supply — one area of life where politics should play no role.

Shopper card records, profiling, and law enforcement

Federal agencies practice profiling

The same software used by grocery marketers to analyze purchase records and predict future behavior is also being used by accountants at the Department of Defense (DOD) to keep tabs on 40,000 DOD employees.[62] When an employee uses his or her "government purchase card" the transaction is analyzed against the employee's personal information and previous purchase history.[63] Then the purchase is compared with profiles of "data patterns that might indicate improper use."[64]

The problem is that the program doesn't always work. Officials admit it needs "some fine tuning" after observing its unsettling tendency to make false accusations.[65] Over a recent three-month test period, the software caused 345 individuals to be put under investigation for making "suspicious purchases," many of which later turned out to be legitimate.[66] Unfortunately, worries over falsely accusing the innocent have done little to dampen the agency's enthusiasm for the data-mining program; the DOD plans to expand its use in coming years.[67]

The DOD will have plenty of company. The IRS may soon "feed data from every entry on every tax return, personal or corporate, through filters to identify patterns of taxpayer conduct."[68] The agency hopes to compile and store detailed information in taxpayer databases that can be sifted through in search of irregularities.[69] Given the insight into household income that eating habits provide, the IRS might find grocery records a tempting target for inclusion in the database. British revenue authorities have already demanded customer purchase records from supermarkets in the U.K. to investigate whether shoppers' spending habits match the lifestyles indicated by their tax returns.[70]

Of course, no one scans a grocery card with the expectation that their data will wind up in the hands of the IRS. Nevertheless, data given to retailers for one purpose has a disquieting tendency to wind up in someone else's hands. Selective Service once came under fire for using a list of children's addresses and birthdays from Farrell's ice cream parlors to mail out reminders about Selective Service registration.[71] Farrell's had originally collected the information to offer free ice cream cones on kids' birthdays.[72]

Profiling by law enforcement

Law enforcement agencies are already making use of shopper card records. DEA agents obtained the supermarket card records of individuals in Arizona to check for large purchases of plastic bags (presumably for packaging drugs).[73] In theory, shopper card records could be used to trigger this type of investigation whenever *any* purchase fits a "suspicious profile." Soccer moms getting ready for a bake sale could someday find themselves face-to-face with federal authorities asking them to justify their Ziploc purchases.

While the notion of federal authorities rifling through customer databases in search of irregularities may seem unbelievable, former president Bill Clinton has suggested that they do just that. Referring to "suspicious behavior," Clinton was recently quoted as saying, "More than 95% of the people that are in the United States at any given time are in the computers of companies that mail junk mail and you can look for patterns there."[74]

If the Police Federation of England and Wales has its way, it will soon be routine for U.K. law enforcement officials to review grocery records in search of "unusual" or "suspicious" behavior. The Federation has called for the more than 300 separate database records that exist on U.K. citizens — ranging from their supermarket purchase records to their driver's license information — to be merged into one super-database for easy access by law enforcement.[75]

Once the data is thus linked, they have asked for "artificial intelligence systems to watch and listen,"[76] around the clock to every activity recorded in the database. If implemented, powerful software programs would analyze records representing virtually every aspect of individuals' lives in painstaking detail. Of course, these systems will rely on profiling to distinguish between "normal" and "suspicious" behavior.

The specter of ethnic profiling looms especially large when it comes to eating patterns, which can reveal information about a shopper's origin, life experiences, and current economic status.[77] In the wake of the September 11th terrorist attacks, federal agents reviewed the shopper card records of the men involved to create a profile of ethnic tastes and supermarket shopping patterns associated with terrorism.[78] It's hard to see how this information could improve national security, however, considering that the eating habits of Middle Eastern terrorists are probably quite similar to those of Middle Eastern schoolteachers and factory workers.

Unfortunately, supermarkets are making little effort to shield their customers from law enforcement fishing expeditions through their databanks; in fact quite the reverse is true. A national supermarket chain recently approached privacy consultant Larry Ponemon for recommendations on how to advise shoppers that it had violated the privacy policy associated with its

continued on page 558

continued from page 539
card.[79] On his own initiative, a company employee had provided "huge swaths" of customer data to law enforcement to aid in the investigation of the terrorist attacks.[80] Ponemon says that such breaches are increasingly common, with a variety of industries routinely "breaking their privacy policies" and sharing customer data with law enforcement "to analyze suspicious activity."[81]

Can government agents be trusted with this data?

By capturing the fundamental profile of each household... supermarket databases provide the government with a close and surreptitious look into the lives and habits of individuals.[82]
- Christine Anthony, Researcher

While government agencies may want to add shopper card information to the ever-widening number of databases they can access for information about citizens, would such information be safe in their hands? Considering tales of corruption, fraud, and shady dealings around the country, the answer may well be "no."

Abuse of data

Law enforcement officials, who clamor for databases on citizens to keep the public safe from crime, are not above abusing the data to commit their own crimes. Data abuse by government officials appears to be widespread. Just a few recent cases include a DEA agent caught selling sensitive records from several different government databases and officials in Las Vegas selling confidential court records.[83]

More than 90 state police employees have been accused of misusing Michigan's Law Enforcement Information Network, including a state trooper who used it to keep tabs on her ex-husband's new girlfriend,[84] and another who obtained the home address of an 18-year-old woman in order to hound her for a date.[85] The abuse reaches as far back as 1983 when the database was used to harass a union representative.[86]

The California Department of Motor Vehicles (DMV) has had a particularly hard time keeping its database secure. Scores of DMV employees have abused their access to sensitive information on the system to help criminals commit identity theft and other crimes.[87] Even after firing 80 employees in a yearlong crackdown, the agency acknowledged in late 2000 that it still has "a very large employee fraud problem."[88]

California DMV and Safeway

The California DMV has been involved in some shady dealings with supermarkets, as well. A few years back Safeway (the nation's 3rd largest grocery chain) sent someone to two rival grocery stores to copy the license plate numbers from 1,000 cars in the other stores' parking lots. For $5,000, the DMV sold Safeway the home address of every individual parked at the competition's lot.[89]

Amazingly, a 1990 California state law allows the DMV to release drivers' residential addresses (but not their names) to anyone who can demonstrate a "legitimate business reason" to request the data.[90] The Safeway transaction was apparently "business as usual" and only came to light when an audit revealed that the DMV failed to obtain a written statement from Safeway promising not to use the information for direct marketing purposes.[91] Had the DMV filled out the paperwork correctly, the transaction would have gone undetected.

Perhaps more disturbing, when Safeway's actions came to light the company made no effort to apologize to the people whose privacy it had violated. Safeway spokeswoman Debra Lambert justified the company's behavior and dismissed privacy concerns saying, "It's only addresses. We keep the data to ourselves. It is never divulged outside of the company."[92]

Somehow I suspect the fact that the company keeps those records to themselves would be scant reassurance to the 1,000 shoppers who had chosen not to do business with Safeway in the first place. Since Safeway aggressively collects data on its own customers through its "Safeway Club Card," shoppers in rival parking lots may have been intentionally trying to keep their shopping habits out of Safeway's reach. It is unconscionable that a government agency would circumvent the desire of its citizens to avoid a particular business by selling their confidential records to marketers, and even more appalling that Safeway seems to place no moral or ethical limits on their data collection practices.

SECTION 3: TECHNOLOGY IS PAVING THE WAY FOR DATA COLLECTION ON AN ENORMOUS SCALE

Cards will become inextricably linked with identity

The ability to match names, addresses, purchasing behavior, and lifestyles all together into one record allows companies to build detailed pictures of people's lives.[93] Grocery card records are already being linked with data from a variety of outside sources. For example, more than 700,000 British shoppers have linked their Tesco grocery cards with the natural gas supplied to their homes,[94] thus necessitating the use of a valid name and home address to obtain the card. Of even greater concern are the links being formed between marketing databases and government identification documents.

As supermarket purchase records become increasingly useful informational commodities for law enforcement, government bureaus, and other entities, the accuracy of the data collected will become an important issue. Though it is currently possible to obtain a supermarket card using anonymous or fictitious information at many supermarkets around the country, this loophole could easily close. With "document fraud" being the new buzzword in law enforcement and legislative circles since September 11th (carrying with it a maximum 15-year prison sentence[95]), it is not hard to envision a day when providing

false information on a private contract or card application could be punishable as "fraud."

Supermarkets may begin tightening up their card application procedures to include identity verification. Though customers may balk, the process could be streamlined and made transparent by offering the option of scanning a government-issued ID card instead of a loyalty card. Not only would this reduce the number of cards in a shopper's wallet, it would simplify the collection of food purchase records for inclusion in government databases.

Such a scheme is not far-fetched. Virginia Congressmen Jim Moran (D-VA) and Tom Davis (R-VA) recently introduced legislation that would require all state driver's licenses and ID cards to contain an embedded computer chip capable of accepting "data or software written to the license or card by non-governmental devices."[96] The mandatory "smart chips"[97] would carry bank and debit card data so that citizens could use their ID cards "for a variety of commercial applications."[98] Barring protests from citizens, the state of New Mexico plans to issue a "smart card" driver's license containing a computer memory chip, a portion of which will be set aside for use by credit card issuers and other commercial service providers.[99]

Supermarket "loyalty" cards would be an obvious application for the high-tech smart cards. As Alan Glass, Senior Vice President of Electronic Commerce at MasterCard International, points out, "A senior citizen could have securely protected medical information, supermarket loyalty programs, social club membership and access, discount programs, a municipal transportation pass, and a library card all stored on a single chip."[100]

To complete the total identity picture, the biometrics industry hopes that security concerns will "advance the day when mass commercial applications of biometrics become routine."[101] Accordingly, supermarkets have begun testing out biometric identification systems on U.S. shoppers. Fingerprint payment technology is already in place at a Thriftway grocery store in Washington,[102] and Kroger, the nation's largest supermarket chain, is testing a fingerprint payment system in Texas.[103] The eventual endpoint of the identification-for-food trend may require transmitting one's shopper ID number through a subdermal computer chip implant, such as the Verichip produced by Applied Digital Solutions.[104] A Florida family recently had these chips surgically embedded in a procedure publicized on national television.[105]

Linking government and private sector databases would provide both with nearly omniscient powers of observation over the consumer-citizen. Such a potent concentration of power and knowledge in so few hands could hardly be expected to operate in the interest of privacy and freedom. Sadly, it may be all too easy to convince shoppers that conducting their commercial transactions by means of a government identity document would be more convenient, or that it might somehow promote national security.

Technologies to monitor shoppers' movements

The trade publications for the loyalty marketing industry offer a unique window of insight into the marketers' long-range goals. The writings of marketing strategists reveal a pervasive, industry-wide mentality that will stop at nothing short of omniscient knowledge of consumers' every move — a goal that can only be achieved through total surveillance. As evidence of this mindset, here are a few of the invasive retail surveillance technologies in use today as described on the companies' websites and in related publications.

The ceiling-mounted store cameras originally installed to prevent shoplifting have been turned to a new use — spying on the average shopper. A market research company called Envirosell uses time-lapse surveillance cameras to record detailed information about consumers as they shop. Unlike stationary camera surveillance, which only records what occurs in a given area, Envirosell's technology singles out *individual shoppers*, identified by body mass or body temperature, and "passes" them from camera to camera to record their movements during the entire shopping trip.[106] The surveillance is so complete that if a shopper lingers for more than a few moments in one spot, a wall-mounted camera may zoom in to peer closely at the individual's face.[107]

Apparently, Envirosell feels it is necessary to collect "hundreds of hours of video tape"[108] in this manner, since customer behaviors such as reading labels are "easier to observe on tape, where they may be repeatedly watched frame by frame, than live."[109] The system also employs unobtrusive on-site researchers called "trackers" to follow shoppers around the store, listening in on and recording their conversations.[110] Envirosell has even stooped to closely scrutinizing the moment-by-moment behavior of customers seated at fast food restaurants and groups interacting in sit-down restaurants, without their knowledge or consent.[111]

A "Frequently Asked Questions" (FAQ) page on Envirosell's website is filled with reassurances apparently designed to soothe the skittish retail executive. It explains, for example, that "according to Federal law, in-store filming in public areas does not constitute an invasion of the privacy of customers or employees,"[112] and asserts that video surveillance is employed by "virtually every retail chain in this country."[113] The FAQ page also offers revealing insight into the company's attitude towards shoppers. Asked, "Do customers know they're being watched?" the website explains that "most shoppers are so intent on the shopping process that they notice very little of what goes on around them. . . . However, when they do notice [the cameras] most people assume that they are for security purposes."[114]

Apparently, Envirosell has no shortage of clients. Fred Meyer, CVS, Trader Joe's, and Wal-Mart are among

the nearly 50 major retailers that have used Envirosell's surveillance system to spy on their customers.[115]

Envirosell is just one of many companies eager to deploy its espionage systems in retail environments. Brickstream Corporation uses in-store video technology and image analysis software to track where customers go and what they do in retail stores and banks.[116] A press release issued by Brickstream and partner company Retek Inc. once boasted, "This solution is transparent to the customer yet yields a wealth of information and customer insight for the retailer," [117] implying that shoppers will have no knowledge of being watched. Point Grey Research markets the Censys3D video surveillance system, which literally draws a line on a time lapse video indicating the exact movements of each person who enters the environment.[118]

Not content to rely on mere surveillance cameras, IBM has developed a thermal tracking system it calls "Footprints" to monitor shoppers.[119] The system uses sensors mounted throughout the store that pick up body heat.[120] The sensors are so precise that they can distinguish between individuals in a group and track the exact path of an individual shopper through the store.[121] It is suggested that the thermal technology be coupled with existing video cameras so that human observers can record sex, age and approximate income group data as well.[122]

A company called ShopperTrak has developed a "traffic counter [that] utilizes an on-board video sensor and multiple high-speed microprocessors to unobtrusively track shoppers' movements."[123] The system, which "literally watches shoppers from overhead," has already been implemented at 6,000 retail locations worldwide and is touted as "discreet" on the company's website.[124]

Another company, KartSaver Inc., mounts tracking devices to shopping carts that communicate via infrared signals to receivers mounted in the store's ceiling.[125] This allows the store to track "the traffic patterns and shopping habits"[126] of individual consumers as they walk around the supermarket. In the covert fashion typical of these companies, KartSaver once boasted in a press release that "most consumers will never even know that the product is being employed."[127]

Hy-Vee Food Stores, one of America's 15 largest grocery chains, recently contracted to have a similar infrared cart-tracking network installed in its Kansas City stores.[128] Klever Marketing, which developed and installed the system, equipped Hy-Vee shopping carts with tracking devices and video screens to better "guide [shoppers'] movements and influence their purchasing decisions."[129]

Klever Marketing suggests that its technology could be linked with frequent shopper card records, since knowing a shopper's complete purchase history, along with his or her precise location in the store, would better enable the supermarket to target the shopper with promotional messages.[130] "I think we have just touched the tip of the iceberg," said a senior Hy-Vee executive.[131] "[This] will be a standard part of our business within the next three to five years."[132] Then, ominously, he added, "I'm not sure any of us know what all the final uses will be."[133]

Semcor Inc., a Microsoft strategic partner in the business of using "geographic information systems"[134] to "track and monitor the movements of vehicles, equipment, wildlife and virtually anything else that moves,"[135] also suggests "inserting mini radio transmitters into shopping carts in your supermarket"[136] to keep track of shoppers.

Bridge Technology, an Arizona corporation, is just one of the many companies that hope to link loyalty cards to wireless communications, global positioning systems (GPS), and Internet technologies to record transactions and collect data from remote and mobile locations on a real-time basis.[137] This technology would enable supermarket cards not only to record what people buy, but where they travel as well.

Even the floor people walk on can be used to surreptitiously gather data on them.[138] Semcor's website advises the use of pressure sensitive floor pads to keep tabs on people as they visit museums, galleries, and zoos.[139] Pressure sensitive flooring may be just the beginning. Students at MIT's Media Lab have developed a system of floor sensors that can identify each place a person has moved within a room over time and exactly where they are at any given moment.[140]

While a shopper may be upset to learn how extensively her local retailer observes customers, imagine her horror at discovering that her favorite boutique is not a store at all, but a carefully designed clandestine consumer research laboratory. One such "store" now exists.[141] The Once Famous boutique in Minneapolis is a 1,800-foot storefront that presents itself to shoppers as a trendy home furnishings store.[142] What shoppers don't know is that the decorative items are merely props to lure them inside the store where they serve as unsuspecting - and unpaid - research subjects.[143] A complex network of cameras and microphones carefully concealed throughout the boutique is used to observe and record each shopper's response to specific items offered for sale.[144] These reactions are later written up and sold to clients of the parent company, who pay anywhere from $15,000 to $100,000 or more for researchers to observe subjects handling their products.[145]

Considering how determined marketers seem to be to watch customers' every move, it may not be long before another Applied Digital Solutions product—the "Digital Angel Monitor," a GPS system that can be worn as a wristwatch to allow anyone to "find a person, animal or object anywhere in the world . . . anytime"[146]—is recommended as the perfect device for collecting consumer data 24 hours a day.

Auto-ID: Tracking everything, everywhere

In 5-10 years, whole new ways of doing things will emerge and gradually become commonplace.

Expect big changes.[147]
- MIT's Auto-ID Center

Supermarket cards and retail surveillance devices are merely the opening volley of the marketers' war against consumers. If consumers fail to oppose these practices now, our long-term prospects may look like something from a dystopian science fiction novel.

A new consumer goods tracking system called Auto-ID is poised to enter all of our lives, with profound implications for consumer privacy. Auto-ID couples radio frequency (RF) identification technology with highly miniaturized computers that enable products to be identified and tracked at any point along the supply chain.[148]

The system could be applied to almost any physical item, from ballpoint pens to toothpaste, which would carry their own unique information in the form of an embedded chip.[149] The chip sends out an identification signal allowing it to communicate with reader devices and other products embedded with similar chips.[150]

Analysts envision a time when the system will be used to identify and track every item produced on the planet.[151]

A number for every Item on the planet

Auto-ID employs a numbering scheme called ePC (for "electronic product code"), which can provide a unique ID for any physical object in the world.[152] The ePC is intended to replace the UPC bar code used on products today.[153]

Unlike the bar code, however, the ePC goes beyond identifying product categories — it actually assigns a unique number to every single item that rolls off a manufacturing line.[154] For example, each pack of cigarettes, individual can of soda, light bulb or package of razor blades produced would be uniquely identifiable through its own ePC number.[155]

Once assigned, this number is transmitted by a radio frequency ID tag (RFID) in or on the product.[156] These tiny tags, predicted by some to cost less than 1 cent each by 2004,[157] are "somewhere between the size of a grain of sand and a speck of dust."[158] They are to be built directly into food, clothes, drugs, or auto-parts during the manufacturing process.[159]

Receiver or reader devices are used to pick up the signal transmitted by the RFID tag. Proponents envision a pervasive global network of millions of receivers along the entire supply chain — in airports, seaports, highways, distribution centers, warehouses, retail stores, and in the home.[160] This would allow for seamless, continuous identification and tracking of physical items as they move from one place to another,[161] enabling companies to determine the whereabouts of all their products at all times.[162]

Steven Van Fleet, an executive at International Paper, looks forward to the prospect. "We'll put a radio frequency ID tag on everything that moves in the North American supply chain," he enthused recently.[163]

The ultimate goal is for Auto-ID to create a "physically linked world" [164] in which every item on the planet is numbered, identified, catalogued, and tracked. And the technology exists to make this a reality. Described as "a political rather than a technological problem," creating a global system "would . . . involve negotiation between, and consensus among, different countries."[165] Supporters are aiming for worldwide acceptance of the technologies needed to build the infrastructure within the next few years.[166]

The implications of Auto-ID

Theft will be drastically reduced because items will report when they are stolen, their smart tags also serving as a homing device toward their exact location.[167]
- MIT's Auto-ID Center

Since the Auto-ID Center was founded at the Massachusetts Institute of Technology (MIT) in 1999, it has moved forward at remarkable speed. The center has attracted funding from some of the largest consumer goods manufacturers in the world, and even counts the Department of Defense among its sponsors.[168] In a mid-2001 pilot test with Gillette, Philip Morris, Procter & Gamble, and Wal-Mart, the center wired the entire city of Tulsa, Oklahoma with radio-frequency equipment to verify its ability to track Auto-ID equipped packages.[169]

Though many Auto-ID proponents appear focused on inventory and supply chain efficiency, others are developing financial and consumer applications that, if adopted, will have chilling effects on consumers' ability to escape the oppressive surveillance of manufacturers, retailers, and marketers. Of course, government and law enforcement will be quick to use the technology to keep tabs on citizens, as well.

The European Central Bank is quietly working to embed RFID tags in the fibers of Euro bank notes by 2005.[170] These tags would allow money to carry its own history by recording information about where it has been, thus giving governments and law enforcement agencies a means to literally "follow the money" in every transaction.[171] If and when RFID devices are embedded in banknotes, the anonymity that cash affords in consumer transactions will be eliminated.

Hitachi Europe wants to supply the tags. The company has developed a smart tag chip that — at just 0.3mm square and as thin as a human hair — can easily fit inside of a banknote.[172] Mass-production of the new chip will start within a year. [173]

Consumer marketing applications will decimate privacy

Radio frequency is another technology that supermarkets are already using in a number of places throughout the store. We now envision a day where consumers will walk into a store, select products whose packages are embedded with small radio frequency UPC codes, and exit the store without ever going through a checkout line or signing their name on a dotted line.[174]
- Jackie Snyder, Manager of Electronic Payments for Supervalu (Supermarkets), Inc., and Chair, Food

Marketing Institute Electronic Payments Committee

Auto-ID would expand marketers' ability to monitor individuals' behavior to undreamt of extremes. With corporate sponsors like Wal-Mart, Target, the Food Marketing Institute, Home Depot, and British supermarket chain Tesco, as well as some of the world's largest consumer goods manufacturers including Proctor and Gamble, Phillip Morris, and Coca Cola[175] it may not be long before Auto-ID-based surveillance tags begin appearing in every store-bought item in a consumer's home.

According to a video tour of the "Home of the Future" and "Store of the Future" sponsored by Proctor and Gamble, applications could include shopping carts that automatically bill consumer's accounts (cards would no longer be needed to link purchases to individuals), refrigerators that report their contents to the supermarket for re-ordering, and interactive televisions that select commercials based on the contents of a home's refrigerator.[176]

Now that shopper cards have whetted their appetite for data, marketers are no longer content to know who buys what, when, where, and how. As incredible as it may seem, they are now planning ways to monitor consumers' use of products within their very homes. Auto-ID tags coupled with indoor receivers installed in shelves, floors, and doorways,[177] could provide a degree of omniscience about consumer behavior that staggers the imagination.

Consider the following statements by John Stermer, Senior Vice President of eBusiness Market Development at ACNielsen:

[After bar codes] [t]he next 'big thing' [was] [f]requent shopper cards. While these did a better job of linking consumers and their purchases, loyalty cards were severely limited...consider the usage, consumer demographic, psychographic and economic blind spots of tracking data.... [S]omething more integrated and holistic was needed to provide a ubiquitous understanding of on- and off-line consumer purchase behavior, attitudes and product usage. The answer: RFID (radio frequency identification) technology.... In an industry first, RFID enables the linking of all this product information with a specific consumer identified by key demographic and psychographic markers....Where once we collected purchase information, now we can correlate multiple points of consumer product purchase with consumption specifics such as the how, when and who of product use.[178]

Marketers aren't the only ones who want to watch what you do in your home. Enter again the health surveillance connection. Some have suggested that pill bottles in medicine cabinets be tagged with Auto-ID devices to allow doctors to remotely monitor patient compliance with prescriptions.[179]

While developers claim that Auto-ID technology will create "order and balance" in a chaotic world,[180] even the center's executive director, Kevin Ashton, acknowledges there's a "Brave New World" feel to the technology.[181] He admits, for example, that people might balk at the thought of police using Auto-ID to scan the contents of a car's trunk without needing to open it.[182] The Center's co-director, Sanjay E. Sarma, has already begun planning strategies to counter the public backlash he expects the system will encounter.[183]

Customers are dehumanized

[T]he consumer is therefore constantly constructed as an exterior object to be captured, studied, reduced and targeted by the operator, in other words, as the enemy of the intelligent machine.[184]
- John Goss, Marketing the New Marketing

What does all of this say about the marketing industry and its attitudes? In their frenzy to manipulate others, marketers have lost their awareness of their fellow human beings as equals, deserving of dignity and respect. Viewed through the distorted lens of loyalty marketing, customers cease to be people; they are transformed into rather stupid domestic animals or laboratory specimens, becoming inventory units to be studied, manipulated, controlled, and exploited to maximize their contribution to the bottom line. Any *feelings* the customer may express about this treatment are dispassionately observed and duly recorded to become fodder for even more analysis, which is then used to inform the next, more thorough iteration of persuasion and control.

While we may be "valued customers," our value is no more than that of chattel, since our true value — our *humanity* — is disregarded. Shopper cards play a key role in fostering this dehumanization in the minds of retailers and marketers. Once consumers are systematically numbered and recorded in the database, the supermarket can finally treat them like any other item in their inventory control system — as impersonal units to be numbered, cataloged, and tracked.

SECTION 4: WORKING TOWARD A SOLUTION

A national organization to oppose supermarket surveillance cards

When I first realized the long term implications of allowing our food purchases to be monitored and recorded, I created a website that grew into CASPIAN, Consumers Against Supermarket Privacy Invasion and Numbering (www.nocards.org). CASPIAN's mission is to educate consumers, condemn marketing practices that invade customers' privacy, and encourage privacy-conscious shopping habits across the retail spectrum. Today, CASPIAN's membership base spans the U.S.A. and our efforts have been featured by numerous media outlets including Kiplinger's Personal Finance magazine, Extra!, the Boston Globe, the Seattle Times, the major television networks, PBS, and local

radio, TV, and newspapers around the country.[185]

CASPIAN believes that individual consumers are ultimately responsible for protecting their own privacy, so we encourage shoppers to become informed, inform others, and "vote with their feet."[186] We also encourage peaceful protests against card programs and other intrusive retail surveillance schemes. We do not advocate legislative solutions to the card problem, having observed a disturbing trend in the past for "data protection laws" to put the data to be protected squarely into the hands of the government.[187]

A common sentiment expressed by new CASPIAN members is, "Thank goodness I found you; I thought I was the only person to feel this way!"[188] And indeed one of CASPIAN's key roles is to encourage privacy-conscious shoppers with the knowledge that they are not alone. Regrettably, many supermarket chains demoralize card opponents by pretending ignorance of the movement to oppose cards and failing to acknowledge the large volume of anti-card complaints they receive.[189]

Arguments against using "fake" or traded cards

Unfortunately, many shoppers think they have found a clever way to bypass the surveillance schemes at their local supermarkets by filling out shopper card applications under false names or trading their grocery cards with others.[190] Though the shopper may think he or she is pulling the wool over the supermarkets' eyes, these tactics actually play right into the marketers' hands.

In a brilliant counter-move, stores not only permit these practices, but may openly encourage them as a way to lull card opponents into participating in the system rather than fighting it. Stores know that the fake name "loophole" removes dissenters from the ranks of the opposition and adds them instead to the army of shoppers standing in line with cards — where they continue to pour money into the store's coffers. The anti-shopper-card movement loses some of its strongest potential allies this way, because shoppers who sign up under fake names or trade cards with others believe they've found "the solution" and no longer have to fight.

Though the choice of where to shop may feel like a decision that only affects the consumer, it is a two-way street. Money that leaves the shopper's wallet winds up in someone else's. By continuing to shop at card stores, consumers contribute their hard-earned grocery money to fund the retail surveillance agenda. They pay for publicists to fight people like me. They pay the salaries of the Catalina Marketing executives who create and peddle these schemes.[191] And they pay for psychologists to analyze the remaining holdouts to find ways to overcome their resistance.

Boycott cards now while there are still alternatives

[One] customer issue is the inertia of the typical consumer. While a segment will always be active and vigilant, the majority will pay less attention to encroachments on their right to privacy.[192]
- Frank Franzak, et al., Journal of Consumer Marketing

Find out just what any people will quietly submit to and you have found out the exact measure of injustice and wrong which will be imposed upon them, and these will continue till they are resisted with either words or blows, or both. The limits of tyrants are prescribed by the endurance of those whom they oppress.[193]
- Fredrick Douglass, Two Speeches

It is surprising that so many people cooperate with the retail surveillance agenda, considering how easy it is to resist. For most shoppers, resisting simply means driving a few extra minutes to a card-free supermarket and paying by cash instead of using a credit card. If everyone who opposed cards decided to shop elsewhere for even a few months, the card stores would soon feel the financial effects and the card programs would crumble.

The time to shop elsewhere is now, while alternatives are plentiful. Two of the nation's largest card-free grocery chains are currently test marketing cards (Albertson's in Dallas/Ft. Worth[194] and Winn-Dixie in Florida and Georgia[195]). If shoppers do not stand firm in boycotting these trials, eventually both chains may implement cards nationwide, leaving towns and cities all over the country stranded with few or no card-free shopping options left.

The longer consumers postpone taking action on the problem, the harder it will be to solve in the future. Eventually, the implementation of fingerprint readers in the supermarket coupled with Auto-ID technology may make the problem so enormous that few will have the strength to resist.

The tide is turning

The good news is that consumers appear to be growing wary of card-based surveillance. Stop & Shop's Curt Avallone revealed that acceptance levels for Stop & Shop's card have dropped from a high of 50% eight years ago to just 40% today.[196] He admits that "people are disappointed in the card and what we've been doing with it"[197] and acknowledges that privacy concerns have become a sticky issue for the company.[198]

American consumers may be poised to take back the ground they have lost. When Albertsons began test-marketing its card program in Texas last year, it was met with fierce opposition by CASPIAN-led shoppers who joined together in a boycott and mounted a peaceful protest against the store.[199] Virtually all of the major media in Dallas (television, newspaper, and radio) discussed the privacy implications of the card and informed shoppers of the movement to oppose it. The media coverage and boycott corresponded with a drop in Albertson's market share in the region.[200] Through continued pressure, CASPIAN hopes to encourage Albertsons to reconsider its plans to introduce the card

elsewhere.

A number of other supermarket chains have dismantled their card programs over the years in response to consumer concerns.[201] These include Raley's (rated America's #1 supermarket chain by Consumer Reports[202]), Wild Oats (the nation's third largest natural food chain by sales[203]), and the H.E.B. Grocery Company of San Antonio (recently called the "most impressive"[204] of U.S. grocery retailers).

Even Britain's fourth largest grocery retailer, Safeway (now unrelated to the U.S. chain of the same name), abandoned its card program in 2000 because of its enormous cost. When the chain re-channeled the approximately $70 million it had been spending annually on cards into lower overall prices,[205] its market share rose 5%.[206] "People don't think [the cards] give value. [But] they'll never get tired of great deals," explained Safeway's chief executive Carlos Criado-Perez.[207]

A message of hope

Though danger is on the horizon, consumers need not feel hopeless, outnumbered, or discouraged. The good news is that the corporations are dependent on their customers, not the other way around. As soon as large numbers of consumers begin to withhold their shopping dollars from stores that engage in shopper surveillance, stores will scramble to regain those dollars through more responsible practices. We must each make the decision to stop funding the beast.

SECTION 5: CONCLUSION

It's not too late to turn back

We all want progress . . . [but] if you're on the wrong road, progress means doing an about-turn and walking back to the right road; and in that case, the man who turns back soonest is the most progressive man... We are on the wrong road. And if that is so, we must go back. Going back is the quickest way on. [208]
- C.S. Lewis, Mere Christianity

Of the many reasons to oppose cards, the future is perhaps the most important. Should our children grow up trained to report their every move, activity, and purchase — even the contents of their every meal — to marketers and government officials? As a nation we must think twice about creating a society where everything we do is monitored, scrutinized, and observed by others. I believe that most Americans feel strongly enough about privacy and freedom to reject the surveillance model of society — and are uncomfortable with the direction we are headed.

The promoters of retail surveillance technology might better spend their time asking more fundamental questions about the societal implications of their work, rather than asking themselves how to convince the public to tolerate the all-encompassing surveillance their systems are likely to spawn.

Even today, supermarket cards have begun to serve a conditioning function to ease the public's concerns over other forms of intrusive registration and surveillance. Consumers' use of grocery cards and, by extension, their implied acceptance of the cards' data collection function, are pointed to as justification whenever more invasive schemes are proposed.

A recent UN report cited "the increasing data collection by the private sector" as possibly the most important factor influencing the public's willingness to surrender data to government entities.[209] The report mentions Catalina Marketing, which has collected billions of rows of data on American shoppers, saying, "the widespread public awareness of private sector profiling may act to actually reduce privacy and confidentiality concerns among the public, if they believe that all information about them is already known."[210]

Among other things, supermarket cards have been used to justify National ID.[211] Alan Simpson, Former Senate Majority Whip, testifying on National ID said, "Every time we try to do something in this area, it's filled with emotion, fear, guilt, and racism. You have to do something, and that something is not any more intrusive than what you get when you go into the [grocery] store and slide your [discount] card."[212]

Instead of using supermarket cards as justification for even more invasive surveillance, we need to remember that surveilling the food habits of millions of human beings is in and of itself tremendously invasive. The fact that large numbers of Americans scan a supermarket card on a regular basis does not detract from this reality.

The future is up to us

While surveillance should not be tolerated in any area of our lives, its application to something as physically intimate and essential for survival as food is particularly repugnant. As long as shoppers continue to allow their eating habits to be recorded, the danger will always remain that laws or political maneuvering will override their stores' privacy policies or ethical standards. The data that supermarkets have quietly collected for nearly a decade has become a tempting target for busybodies of all stripes.

There will always be those who believe the potential societal benefits of surveillance schemes outweigh the risks of abuse. However, though there is ample evidence that the supposed security "benefits" of mass surveillance are quite doubtful,[213] the risks of unchecked government control are very real and not to be discounted.[214] As the police and other agents of the state increasingly tap the power of the retail sector's growing arsenal of sophisticated surveillance technologies, we may soon find ourselves in the totalitarian nightmare described by George Orwell in *1984*. It is up to each of us to ensure that comprehensive, all-knowing surveillance systems are returned to the scrap heap of history's bad ideas before it is too late to turn back.

Even though most citizens are unaware of Auto-ID and plans for omniscient police and UN databases, virtually everyone has heard of the lowly supermarket card. And here,

finally, is one useful purpose cards can serve: as a wake up call to the public. Americans must take a second look at the cards in their wallets and on their key chains, recognizing that they represent only the most visible component of a massive push toward global surveillance being driven by the retail sector. Cards are just one symptom of an advancing disease that, left unchecked, will almost certainly prove fatal to privacy — and may ultimately threaten freedom itself.

Katherine Albrecht is the founder and director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), a national grass-roots consumer group dedicated to fighting supermarket "loyalty" or frequent shopper cards. CASPIAN's efforts are dedicated to educating consumers, condemning marketing practices that invade customers' privacy, and encouraging privacy-conscious shopping habits across the retail spectrum. Formed in 1999, CASPIAN has since reached millions of American consumers with its pro-privacy message.

Katherine Albrecht holds a Master's degree in Education from Harvard University and a Bachelor's degree in International Marketing.

Appendix 1: Grocery Card Programs

This chart lists the card status of a number of chains owned by the ten largest grocery retailers based on 2001 sales

RANKING BY 2000 SALES[215]	COMPANY	CARD STATUS	PROGRAM NAME
1) $51b	THE KROGER COMPANY		
	• Kroger, Hilander, Owen's, Pay Less, Dillons, Gerbes	CARD	Plus Card
	• City Market	CARD	Value Card
	• King Soopers	CARD	SooperCard
	• Ralph's	CARD	Club Card
	• Fry's	CARD	VIP Card
	• Smith's	CARD	Fresh Values Rewards Card
	• Food 4 Less	NO CARD	Food 4 Less is a "no-frills" grocery store where shoppers bag their own groceries.
	• Fred Meyer	NO CARD	Kroger customer service representatives say that Fred Meyer may get a card program in late 2002.
	• Quality Food Centers (QFC)	CARD	Advantage Card
2) $38b	ALBERTSON'S INC.		
	• Albertson's	TESTING CARD	"Preferred Savings Card" introduced in Dallas/Ft. Worth, Texas November 2001
	• Acme	CARD	Super Card
	• Jewel	CARD	Preferred Card
3) $34b	SAFEWAY INC.		
	• Safeway	CARD	Club Card
	• Dominick's	CARD	Fresh Values Card
	• Pavilions	CARD	ValuePlus Card
	• Randall's	CARD	Remarkable Card
	• Tom Thumb	CARD	Rewards Card
	• Vons	CARD	VonsClub Card
4) $23b	AHOLD USA, INC.		
	• Bi-Lo, Giant, Tops	CARD	Bonuscard / Bonus Card
	• Stop & Shop	CARD	Stop & Shop Card
5) $20b	WAL-MART SUPERCENTERS	NO CARD	
6) $18b	SAM'S CLUB	MEMBER CARD	Membership card tracks purchases but there is no "two-tiered" pricing
7) $18b	COSTCO WHOLESALE GROUP	MEMBER CARD	Membership card tracks purchases but there is no "two-tiered" pricing
8) $15b	DELHAIZE AMERICA		
	• Food Lion	CARD	MVP Card
	• Kash n' Karry	CARD	Preferred Customer Club
	• Hannaford (Shop 'n Save)	NO CARD	
9) $15b	PUBLIX SUPER MARKETS, INC.	NO CARD	
10) $13b	WINN-DIXIE STORES, INC.	TESTING CARD	"Customer Reward Card" introduced in Florida and SE Georgia March 2002